UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,344	08/16/2001	Massimiliano Antonio Poletto	12221-004001	2635

26161 7590 06/26/2007
FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
06/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/931,344	POLETTO ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 February 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-39 have been re-examined and are pending.

2. This is a Non-Final rejection.

3. In view of the Appeal Brief filed on 2/13/2007, PROSECUTION IS HEREBY REOPENED. A Non-Final is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

4. Claims 1, 16, and 29 are provisionally rejected on the ground of nonstatutory double patenting over claims 1, 9, 18, and 21 are of copending Application No. 09/931,291. This is a provisional double patenting rejection since the conflicting claims have not yet been patented.

The subject matter claimed in the instant application is fully disclosed in the referenced copending application and would be covered by any patent granted on that copending application since the referenced copending application and the instant application are claiming common subject matter, as follows:

Claims 1, 16, and 29 of '344 recites a gateway disposed between a data center and a network for thwarting denial of service attacks on the data center Claims 1, 9, 18, and 21 of '291 reciting a computer system to coordinate

thwarting attacks on a data center that is coupled to a network and further discloses the process to identify gateways on the monitoring network that are resources of malicious traffic destined for the data center. Thus, '344 and '291 obviously uses gateways for monitoring attacks towards the data center.

Both '344 and '291 recites communication of statistics collected from the monitoring process that obviously involves network traffic, attacks, etc. Further, '344 disclose the gateway comprises a computing device disposed between a data center and a network where the gateway is obviously separate or physically apart from the data center and the network because the gateway is disposed between the data center and the network. This obviously reads on '291 where plurality of monitors is physically separate network from the network that the data center is couple to.

Claims 1, 16, and 29 of '344 recite a filtering process to insert filters on network devices to filter out packets that deems to be part of an attack. Claims 1, 9, 18, and 21 of '291 recites network flows collected by plurality of monitors and analyzing the statistical data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic. The plurality of monitors of '291 is obviously a broader variation to the filters of '344 because both applications claim a filtering process but '291 analyzes the traffic and '344 filters out the traffic that is considered an attack or malicious. Therefore, it would have been obvious the limitations of '344 reads on '291

because both applications monitors network traffic to thwart attacks on a data center.

5. Claims 1, 16, and 29 are provisionally rejected on the ground of nonstatutory double patenting over claims 1, 3, and 4 are of copending Application No. 10/066,252. This is a provisional double patenting rejection since the conflicting claims have not yet been patented.

As for '344, claim 1 recites a gateway disposed between a data center and a network for thwarting denial of service attacks on the data center. Claim 16 and 29 recites a victim site that is being protected from denial of service attacks and claim 16 additionally recites disposing a gateway between the victim site and a network. Thus, the victim site can broadly be given as a data center because both are being protected from denial of service attacks.

As for '291, claim 1 recites a device coupled to physical links between the data center and a network with the device disposed to examine traffic entering or leaving that data center on the couple physical links and collect statistical information.

The device of '291 can broadly interpret as a gateway device of '344 because both devices are coupled between a data center and a network for monitoring and collecting traffic. Further, the difference between claims 1, 3, and 4 of '291 to claims 1, 16, and 19 of '344 is that '344 do not include physical links. Physical links obviously is for one device to couple to other

devices such as a gateway device coupled to physical links to the data center of claim 1 of '344 in order for communication of traffic to monitor the traffic of the network. Therefore, it would have been obvious the combined limitations from claims 1, 3 and 4 of '291 reads on claims 1, 16, and 19 of '344 because there includes monitoring, examining, and collecting network traffic for thwarting denial of service attacks on the data center.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pearson (US 6,990,591), and further in view of Cheriton (US 7,120,931).

As per claim 1:

discloses gateway device disposed between a data center and a network for thwarting denial of service attacks on the data center, the gateway device comprises: a computing device comprising:

a monitoring process that monitors network traffic through the gateway; **(col.6, lines 6-19; Pearson discloses a communication device 106 is also referring to a gateway, firewall, or other devices that communicates data between one or more ports. The firewall and intrusion detection functionality of communication device protects the resources of LAN from potential hackers. Thus, the claimed gateway will hereinafter refer to the communication device 106.)**

a communication process that communicate statistics collected in the gateway from the monitoring process **(col.8, lines 10-15 and col.19, lines 45-50)** with a control center and that receives queries or instructions from the control center; **(col.7, lines 55-62; col.9, lines 11-17; FIG.1 (controller 112); and col.20, lines 40-50; Pearson discloses the remoter monitoring center (RMC) 130 comprises several components that provide functionality for carrying out various tasks (col.6, lines 42-55). The RMC is the claimed control center where the communication device carries out communications from the RMC (col.15, lines 52-65 and col.16, lines 26-29).)**

and [a filtering process to insert filters on network devices to filter out packets] that the gateway deems to be part of an attack. **(col.9, lines 11-16 and col.16, lines 36-53)**

Pearson discloses a predetermined level of network security, that is, monitoring for certain predetermined responses to such threats, may be

established (col.10, lines 56-64) where the RMC is operative in response to the selection to one of the selectable security levels to automatically configure the communication device to monitor for certain predetermined threats and to provide certain predetermined responses (co.11, lines 7-12). Further, Pearson discloses remote agents may be software application programs for classifying and handling identified security risks (col.18, lines 21-24). Thus, Pearson suggests selectively configure to monitor certain threats and of security levels. Pearson seems to suggest the claimed a filtering process to filter out packets by an intrusion detector and that all communications are analyzed and compared to the list of known attacks (col.9, lines 11-16 and col.16, lines 36-53). However, Pearson did not particularly discusses a filtering process to insert filters on network devices to filter out the threats.

Cheriton discloses propagating filters to an upstream device comprises generating a filter at a first network device where a computer program product for generating filters based on analyzed network flows generally comprises code that analyzes harmful network flows to prevent network flows from passing through the network device (col.2, lines 29-43). Cheriton discloses a filter is inserted into a firewall located between a router and plurality of servers so data incoming is filtered to reduce the possibility of problems in the network (col.3, lines 38-53). The firewall is preferably a packet filtering firewall but may also be a proxy (application) firewall (col.5, lines 20-25). Network device may also be routers and switches (col.3, lines 58-63 and col.5, lines 26-30). Cheriton

discloses that once a group of packets are identified as harmful, the corresponding network flows can be analyzed to further refine the filter and therefore, instead of filtering out all data arriving from the identified organization, only destructive packets received from the actual attacker are dropped (col.7, lines 18-24 and 32-65).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Pearson with Cheriton to teach inserting the filter in a network device such as a firewall because analyzes harmful network flows to prevent network flows from passing through the network device (col.2, lines 29-43) and data incoming is filtered to reduce the possibility of problems in the network (col.3, lines 38-53).

As per claim 2: See Pearson on col.3, lines 59-65 and col.12, lines 30-33; discussing the communication process couples to a dedicated link to communicate with the control center over a hardened network.

As per claim 3: See Pearson on col.1, lines 52-60; discussing the monitoring process in the gateway samples network packet flow in the network.

As per claim 4: See Pearson on col.15, lines 18-20 and col.16, lines 34-36; discussing the gateway is adaptable to be physically deployed in line in the network.

As per claim 5: See Cheriton on col.2, lines 50-63 and col.5, lines 26-30; discussing the gateway is adaptable to dynamically install filters on nearby routers.

As per claim 6: See Pearson on col.18, lines 51-67; discussing the monitoring process detects IP traffic and determines levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.

As per claim 7: See Pearson on col.17, lines 35-47 and Cheriton on col.8, lines 1-44; discussing the monitoring process detects Internet Protocol (IP) traffic and determines levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses.

As per claim 8: See Pearson on col.17, lines 47-47 and Cheriton on col.6, lines 10-18; discussing monitoring process detects Internet Protocol (IP) traffic and determines levels of Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packets to unused ports.

As per claim 9: See Pearson on col.8, lines 16-25 and Cheriton on col.8, lines 1-44; discussing monitoring process detects IP traffic and determines levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

As per claim 10: See Pearson on col.10, lines 33-38 and Cheriton on col.8, lines 30-44; discussing monitoring process detects sustained rate higher than plausible for a human user over a persistent HTTP connection.

As per claim 11: See Pearson on col.11, lines 8-12 and Cheriton on col.7,

lines 32-65; discussing monitoring process maintains statistical summary information of traffic over different periods of time and at different levels of detail.

As per claim 12: See Cheriton on col.5, lines 20-25 and col.7, lines 32-col.8, line 10; discussing monitoring process maintains statistics on parameters including source and destination host or network addresses, protocols, types of packets, number of open connections or of packets sent in either direction.

As per claim 13: See Pearson on col.8, lines 10-32 and col.17, lines 1-10; discussing monitoring process has configurable thresholds and issues a warning when one of the measured parameters exceeds the corresponding threshold.

As per claim 14: See Pearson on col.11, lines 31-35; discussing monitoring process logs packets.

As per claim 15: See Pearson on col.11, lines 40-57 and col.18, lines 22-24; discussing monitoring process logs specific packets identified as part of an attack to enable an administrator to identify important properties of the attack.

As per claim 16:

method of protecting a victim site during a denial of service attack, comprises:

disposing a gateway device between the victim site and a network; **(col.6, lines 6-19; Pearson discloses a communication device 106 is also referring to a gateway, firewall, or other devices that communicates data between**

one or more ports. The firewall and intrusion detection functionality of communication device protects the resources of LAN from potential hackers. Thus, the claimed gateway will hereinafter refers to the communication device 106.)

monitoring network traffic through the gateway and measuring heuristics of the network traffic to provide statistics network traffic; **(col.8, lines 10-15 and col.19, lines 45-50)**

communicating the statistics collected in the gateway to a control center; **(col.7, lines 55-62; col.9, lines 11-17; FIG.1 (controller 112); and col.20, lines 40-50; Pearson discloses the remoter monitoring center (RMC) 130 comprises several components that provide functionality for carrying out various tasks (col.6, lines 42-55). The RMC is the claimed control center where the communication device carries out communications from the RMC (col.15, lines 52-65 and col.16, lines 26-29).)**

and filtering out packets that the gateway or control center deems to be part of an attack. **(col.9, lines 11-16 and col.16, lines 36-53; Pearson seems to suggest the claimed a filtering process to filter out packets by an intrusion detector and that all communications are analyzed and compared to the list of known attacks.)**

Pearson discloses a predetermined level of network security, that is, monitoring for certain predetermined responses to such threats, may be established (col.10, lines 56-64) where the RMC is operative in response to the

selection to one of the selectable security levels to automatically configure the communication device to monitor for certain predetermined threats and to provide certain predetermined responses (co.11, lines 7-12). Further, Pearson discloses remote agents may be software application programs for classifying and handling identified security risks (col.18, lines 21-24). Thus, Pearson suggests selectively configure to monitor certain threats and of security levels. However, Pearson did not particularly discusses a filtering out packets that the gateway or control center deems to be part of an attack.

Cheriton discloses propagating filters to an upstream device comprises generating a filter at a first network device where a computer program product for generating filters based on analyzed network flows generally comprises code that analyzes harmful network flows to prevent network flows from passing through the network device (col.2, lines 29-43). Cheriton discloses a filter is inserted into a firewall located between a router and plurality of servers so data incoming is filtered to reduce the possibility of problems in the network (col.3, lines 38-53). The firewall is preferably a packet filtering firewall but may also be a proxy (application) firewall (col.5, lines 20-25). Network device may also be routers and switches (col.3, lines 58-63 and col.5, lines 26-30). Cheriton discloses that once a group of packets are identified as harmful, the corresponding network flows can be analyzed to further refine the filter and therefore, instead of filtering out all data arriving from the identified

organization, only destructive packets received from the actual attacker are dropped (col.7, lines 18-24 and 32-65).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Pearson with Cheriton to teach inserting the filter in a network device such as a firewall because analyzes harmful network flows to prevent network flows from passing through the network device (col.2, lines 29-43) and data incoming is filtered to reduce the possibility of problems in the network (col.3, lines 38-53).

As per claim 17: See Pearson on col.3, lines 59-65 and col.12, lines 30-33; discussing communicating occurs over a dedicated link to the control center via a hardened network.

As per claim 18: See Pearson on col.1, lines 52-60; discussing monitoring samples network packet flow in the network.

As per claim 19: See Pearson on col.15, lines 18-20 and col.16, lines 34-36; discussing the gateway is physically deployed in line in the network.

As per claim 20: See Cheriton on col.2, lines 50-63 and col.5, lines 26-30; discussing filtering further comprises: dynamically installing filters on nearby routers via an out of band connection.

As per claim 21: See Pearson on col.18, lines 51-67; discussing monitoring further comprises: detecting IP traffic and determining levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.

As per claim 22: See Pearson on col.17, lines 35-47 and Cheriton on col.8, lines 1-44; discussing monitoring further comprises: detecting Internet Protocol (IP) traffic and determining levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses.

As per claim 23: See Pearson on col.17, lines 47-47 and Cheriton on col.6, lines 10-18; discussing monitoring further comprises: detecting Internet Protocol (IP) traffic and determining levels of Transport Control Protocol (TCP) or User Datagram Protocol UDP packets to unused ports.

As per claim 24: See Pearson on col.8, lines 16-25 and Cheriton on col.8, lines 1-44; discussing monitoring further comprises: detecting IP traffic and determines levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

As per claim 25: See Pearson on col.10, lines 33-38 and Cheriton on col.8, lines 30-44; discussing monitoring further comprises: detecting a sustained rate of reload requests that is higher than plausible for a human user over a persistent HTTP connection.

As per claim 26: See Cheriton on col.5, lines 20-25 and col.7, lines 32-col.8, line 10; discussing monitoring further comprises: logging statistics on parameters including source and destination host or network addresses, protocols, types of packets, number of open connections or of packets sent in

either direction.

As per claim 27: See Pearson on col.8, lines 10-32 and col.17, lines 1-10; discussing monitoring further comprises: issuing a warning to the control center when one of the measured parameters exceeds a corresponding configurable threshold.

As per claim 28: See Pearson on col.11, lines 40-57 and col.18, lines 22-24; discussing monitoring further comprises: logging specific packets identified as part of an attack to enable an administrator to identify important properties of the attack.

As per claim 29:

computer program product residing on a computer readable medium for protecting a victim site during a denial of service attack, comprises instructions for causing a computer device coupled at an entry to the site to:

monitor network traffic sent to the victim site and measure heuristics of the network traffic to provide statistics on the network traffic; **(col.6, lines 6-19; Pearson discloses a communication device 106 is also referring to a gateway, firewall, or other devices that communicates data between one or more ports. The firewall and intrusion detection functionality of communication device protects the resources of LAN from potential hackers. Thus, the claimed gateway will hereinafter refers to the communication device 106.)**

communicate statistics collected **(col.8, lines 10-15 and col.19, lines 45-50)** in the computer device to a control center; and **(col.7, lines 55-62; col.9, lines 11-17; FIG.1 (controller 112); and col.20, lines 40-50; Pearson discloses the remoter monitoring center (RMC) 130 comprises several components that provide functionality for carrying out various tasks (col.6, lines 42-55). The RMC is the claimed control center where the communication device carries out communications from the RMC (col.15, lines 52-65 and col.16, lines 26-29).)**

filter out packets that the device or control center deems to be part of an attack. **(col.9, lines 11-16 and col.16, lines 36-53; Pearson seems to suggest the claimed a filtering process to filter out packets by an intrusion detector and that all communications are analyzed and compared to the list of known attacks.)**

Pearson discloses a predetermined level of network security, that is, monitoring for certain predetermined responses to such threats, may be established (col.10, lines 56-64) where the RMC is operative in response to the selection to one of the selectable security levels to automatically configure the communication device to monitor for certain predetermined threats and to provide certain predetermined responses (co.11, lines 7-12). Further, Pearson discloses remote agents may be software application programs for classifying and handling identified security risks (col.18, lines 21-24). Thus, Pearson suggests selectively configure to monitor certain threats and of security levels.

However, Pearson did not particularly discusses a filtering out packets that the gateway or control center deems to be part of an attack.

Cheriton discloses propagating filters to an upstream device comprises generating a filter at a first network device where a computer program product for generating filters based on analyzed network flows generally comprises code that analyzes harmful network flows to prevent network flows from passing through the network device (col.2, lines 29-43). Cheriton discloses a filter is inserted into a firewall located between a router and plurality of servers so data incoming is filtered to reduce the possibility of problems in the network (col.3, lines 38-53). The firewall is preferably a packet filtering firewall but may also be a proxy (application) firewall (col.5, lines 20-25). Network device may also be routers and switches (col.3, lines 58-63 and col.5, lines 26-30). Cheriton discloses that once a group of packets are identified as harmful, the corresponding network flows can be analyzed to further refine the filter and therefore, instead of filtering out all data arriving from the identified organization, only destructive packets received from the actual attacker are dropped (col.7, lines 18-24 and 32-65).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Pearson with Cheriton to teach inserting the filter in a network device such as a firewall because analyzes harmful network flows to prevent network flows from passing through the network device (col.2, lines 29-43) and data incoming is filtered to reduce the possibility of problems

in the network (col.3, lines 38-53).

As per claim 30: See Pearson on col.1, lines 52-60; discussing sample network traffic flow.

As per claim 31: See Cheriton on col.2, lines 50-63 and col.5, lines 26-30; discussing instructions to filter further comprise instructions to: dynamically install filters on nearby routers via an out of band connection.

As per claim 32: See Pearson on col.18, lines 51-67; discussing instructions to monitor further comprise instructions to: detect IP traffic; and determine levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.

As per claim 33: See Pearson on col.17, lines 35-47 and Cheriton on col.8, lines 1-44; discussing instructions to monitor further comprise instructions to: detect Internet Protocol (IP) traffic; and determine levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses.

As per claim 34: See Pearson on col.17, lines 47-47 and Cheriton on col.6, lines 10-18; discussing instructions to monitor further comprise instructions to: detect Internet Protocol (IP) traffic; and determine levels of Transport Control Protocol (TCP) or User Datagram Protocol UDP packets to unused ports.

As per claim 35: See Pearson on col.8, lines 16-25 and Cheriton on col.8, lines 1-44; discussing instructions to monitor further comprises instructions

to: detect IP traffic; and determine levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

As per claim 36: See Pearson on col.10, lines 33-38 and Cheriton on col.8, lines 30-44; discussing instructions to monitor further comprises instructions to: detect a sustained rate of reload requests that is higher than plausible for a human user over a persistent HTTP connection.

As per claim 37: See Cheriton on col.5, lines 20-25 and col.7, lines 32-col.8, line 10; discussing instructions to monitor further comprises instructions to: log statistics on parameters including source and destination host or network addresses, protocols, types of packets, number of open connections or of packets sent in either direction.

As per claim 38: See Pearson on col.8, lines 10-32 and col.17, lines 1-10; discussing instructions to monitor further comprises instructions to: issue a warning to the control center when one of the measured parameters exceeds a corresponding configurable threshold.

As per claim 39: See Pearson on col.11, lines 40-57 and col.18, lines 22-24; col.7, lines 43-55; discussing instructions to cause the processor to receive communications from a control center to deliver data pertaining to the types of traffic passing through the gateway.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LH

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100